# From imprecise probability laws to fault tree analysis

Christelle Jacob[1,2] *, Didier Dubois[2], and Janette Cardoso[1]

[1] Institut Supérieur de l'Aéronautique et de l'Espace (ISAE), DMIA department, Campus Supaéro, 10 avenue Édouard Belin - Toulouse
[2] Institut de Recherche en Informatique de Toulouse (IRIT), ADRIA department, 118 Route de Narbonne 31062 Toulouse Cedex 9, France.
{jacob@isae.fr,dubois@irit.fr,cardoso@isae.fr}

**Abstract.** Reliability studies and system health predictions are mostly based on the use of probability laws to model the failure of components. Behavior of the components of the system under study is represented by probability distributions, derived from failure statistics. The parameters of these laws are assumed to be precise and well known, which is not always true in practice. Impact of such imprecision on the end result can be crucial, and requires adequate sensitivity analysis. One way to tackle this imprecision is to bound such parameters within an interval. This paper investigates the impact of the uncertainty pervading the values of law parameters, specifically in fault tree based Safety analysis.

**Key words:** fault trees, Imprecise probabilities, Interval analysis

## 1 Introduction

This work takes place in the context of an Airbus project called @$MOST$. The main aim of the @$MOST$ project is to improve the schedule of operational and maintenance activities of the aircrafts. This is achieved by using some extended safety models and by predicting the expected failures. These predictions are based upon the safety analysis of underlying system models.

One of the objectives of safety analysis is to evaluate the probability of undesired events. In our previous work [1], we studied how to evaluate the imprecision of this probability when the undesired event is described by a fault tree, and the probabilities of elementary events are imprecise numbers. In this approach, the fault tree is a graphical representation of a Boolean formula $F$, representing all the conditions of occurrence of the undesired event under study, as a function of some atomic events. Those atomic events represent the failures of the components of the system, or possibly some of its configuration states. All of them are supposed to be stochastically independent. Then the probability of the undesired event can be computed from the ones of the atomic events, by

* C. Jacob has a grant supported by the @MOST Prototype, a joint project of Airbus, IRIT, LAAS, ONERA and ISAE.

means of Binary Decision Diagrams (BDDs) [3]: that allows an easy probability computation for very large Boolean functions.

In safety analysis, as well in reliability studies, the probabilities of the atomic events are time-dependent, and generally described by means of some standard probability distributions [4], e.g. exponential or Weibull law. Their parameters are supposed to be precisely known numbers, but actually, they generally come from statistical observations of failure times. They are derived by means of data fitting methods and regression analysis: for example, the paper [5] explains how to use different methods, like least squares or the actuary method, in order to find the best parameters of a Weibull law that fit some samples.

In this paper, we investigate the impact of imprecision in parameters of probability distributions commonly used in safety analysis, by using intervals values for the parameters. First of all, we study the impact on the probability distributions themselves: p-boxes [6] are obtained, i.e. minimum and maximum probability distributions bounding the real one. In a second step, an extension of the algorithm described in paper [1] is used to evaluate the imprecise probability of a Boolean formula depending on several p-boxes. In this work, we compute the output p-box attached to undesired events.

The paper is organized as follow: section 2 introduces the basic concepts of reliability. Sections 3 and 4 present the resulting ranges of the cumulative distribution of an atomic event for, respectively, exponential law and Weibull law. At last, section 5 explains the computation of the range of undesired event probability across time (cumulative distribution), in function of the distributions of the atomic events leading to this undesired event. A case study illustrates this section. Finally, the last section presents some conclusions and future work.

## 2 Basics of Reliability study

The *reliability* $R(t)$ of a system, also called the *survival function*, is the probability that the system does not fail before time $t$. It can be expressed as:

$$R(t) = P(T > t) \tag{1}$$

where $T$ is a random variable representing the *failure date*.

The *probability of failure* of a system before time $t$, $F_T(t) = P(T \leq t)$, is the complement of its reliability:

$$F_T(t) = 1 - R(t) \tag{2}$$

$F_T(t)$ is called *failure distribution*.

The *failure density function* $f_T(t)$ expresses the probability that the system fails between $t$ and $t + dt$:

$$f_T(t)dt = P(t \leq T < t + dt) \tag{3}$$

The *failure rate* $\lambda$ of a system is the frequency of its failure. It is a function of the system health state, and in general it is time dependent. $\lambda$ is often considered

as proportional to the probability that a failure occurs at a specified time point $t$, given that no failure occurred before this time:

$$\lambda(t)dt = P(t \leq T \leq t + dt \mid T > t) \tag{4}$$

This conditional probability can be written as:

$$\lambda(t)dt = \frac{f_T(t)dt}{R(t)} = \frac{-R'(t)}{R(t)}, \tag{5}$$

where $R'(t)$ is the derivative of $R(t)$ with respect to the time.

The solution of this differential equation is:

$$\ln(R(t)) = \int_0^t \lambda(u)du + c, \text{where } c \text{ is a constant.} \tag{6}$$

Hence, the reliability expressed in terms of the failure rate has the expression:

$$R(t) = e^{-\int_0^t \lambda(u)du} \tag{7}$$

In the following text, we will present two particular cases of failure rates in equation (7), leading to the following distributions:

- exponential distribution
- Weibull distribution

Furthermore, we will study the impact of the lack of knowledge about failure rates on those distributions.

In reliability studies, the probabilities of all events are assumed to be well known, which is not always verified in practice. Making this assumption has shown some limitation, therefore, some researchers started to work on other methods, using intervals instead of precise values. Utkin and Coolen, for example, worked on imprecise reliability using imprecise probability theory, with upper and lower expectations instead of a single probability value [2]. They studied imprecise monotonic fault trees, and also the impact of some components failure over the system under study by mean of imprecise importance measures.

In this paper, the goal is to compute the probability distribution of an undesired event described by any binary fault tree, monotonic or not. Those kinds of fault trees are often met in software using automatic fault tree generation, or systems with reconfiguration states. The impact of imprecision about the distribution of the undesired event depends on the architecture of the system, and on the imprecision about the parameters of the probability distributions of its elementary components. Hence, the first step is to study the impact of imprecise parameters on the commonly used probability distributions.

## 3 The exponential distribution

Recall that the reliability analysis of an aircraft takes into account, among others, the electronic components. Their probabilities of failure are modeled with constant failure rates, because they do not have any burn-in nor any wear-out periods, respectively at their beginning and their end of life. Moreover, when the failure rate is constant, $\lambda(t) = \lambda$, equation (7) becomes $R(t) = e^{-\lambda t}$, that is an exponential distribution.

The probability density function is given by:

$$f_T(t) = \lambda e^{-\lambda t} \tag{8}$$

And is represented in Fig. 1.a). Its cumulative distribution, depicted in Fig. 1.b) is given by:

$$F_T(t) = 1 - e^{-\lambda t} \tag{9}$$

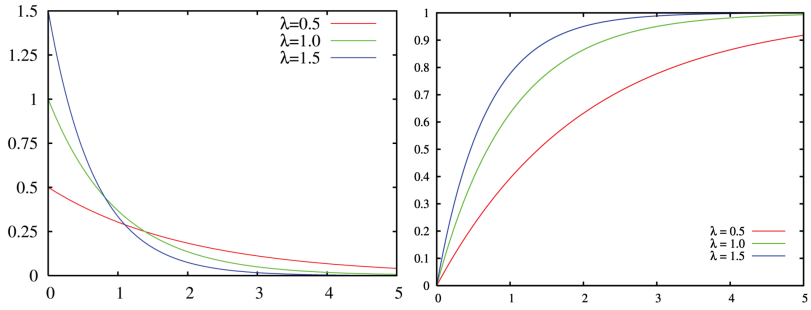



**Fig. 1.** a) Exponential density function b) Cumulative distribution

### 3.1 Exponential law with imprecise failure rate

If the only information available about the failure rate $\lambda$ is an interval containing it, then there are different probability distributions representing the failure of the component, as will be presented in the sequel.

The goal is to find the range of the cumulative distribution, when the failure rate is imprecise: $\lambda \in [\underline{\lambda}, \overline{\lambda}]$. In interval analysis, knowing the monotonicity of a function makes the determination of its range straightforward.

The function $1 - e^{-\lambda t}$ is strictly increasing with $\lambda$, hence the range of the cumulative distribution, when $\lambda$ is varying, for every $t > 0$ and $\lambda > 0$, is given by the expression:

$$F_T(t) = \{1 - e^{-\lambda t}, s.t.\ \lambda \in [\underline{\lambda}, \overline{\lambda}]\} = [1 - e^{-\overline{\lambda} t}, 1 - e^{-\underline{\lambda} t}] \tag{10}$$

The range of the cumulative distribution with respect to some values of $\lambda$ and in time interval $t = [0, 10]$ is represented in Fig. 2.a).

For the probability density function, it is a little bit more complex. The derivative with respect to $\lambda$ of the function $f_T(t)$ is:

$$\frac{\partial}{\partial \lambda} f_T(t) = (1 - \lambda t)e^{-\lambda t} \tag{11}$$

This means that the function will be increasing with respect to $\lambda$ when $\lambda t < 1$, and decreasing otherwise. The range of the function will depend on $\lambda$ and $t$, as illustrated on Fig. 2.b).

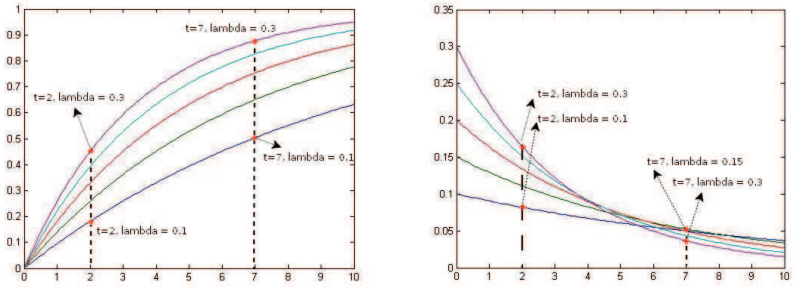



**Fig. 2.** a) Range of the cumulative distribution b) Range of the probability distribution ($0.1 < \lambda < 0.3$, $0 < t < 10$)

In the following, we give different interpretations of the probability of failure of a component, as used in fault tree analysis.

### 3.2 Occurrence of an atomic failure before time $t$

In the quantitative analysis of a safety model, each component (or type of component) of this model will have its own failure rate, and its own failure probability. The main goal of this analysis is to ensure that, at each time $t$, the probability that the system has failed remains below a certain value. Hence, the cumulative distribution will be the one used for our computations, since it represents the probability of failure of a component or system before time $t$.

So when the parameter $\lambda$ is imprecise, and its possible values are known to lie within the interval $[\underline{\lambda}, \overline{\lambda}]$, the probability distribution will be contained in the p-box [6]:

$$\{P, P(T < t) \in [1 - e^{-\overline{\lambda}t}, 1 - e^{-\underline{\lambda}t}]\} \tag{12}$$

The p-box contains more probability distributions than those with an exponential distribution. However it is enough to use the p-box when computing probability bounds of events of the form $T < t$.

### 3.3 Occurrence of an atomic failure between $t_1$ and $t_2$

In some cases, it can also be interesting to compute the probability that the event will occur between two dates $t_1$ and $t_2$. This can be expressed as the

conditional probability $t_1 < T < t_2$ given that $T$ does not occur before $t_1$:

$$P(T < t_2 | T \geq t_1) = \frac{e^{-\lambda t_1} - e^{-\lambda t_2}}{1 - e^{-\lambda t_1}} \tag{13}$$

When $\lambda \in [\underline{\lambda}, \overline{\lambda}]$, the partial derivative of $P(T < t_2 | T \geq t_1)$ with respect to $\lambda$ must be computed in order to find the p-box of the probability distribution.

$$\frac{\partial}{\partial \lambda} P(T < t_2 | T \geq t_1) = \frac{t_2 e^{-\lambda t_2} - t_1 e^{-\lambda t_1}}{(1 - e^{-\lambda t_1})^2} \tag{14}$$

By noticing that the function $xe^{-\lambda x}$ is decreasing with $x$ when $\lambda$ is fixed, we can deduce that $\frac{\partial}{\partial \lambda} P(T < t_2 | T \geq t_1)$ is strictly negative. Hence, the p-box containing the probability that the event occurs between $t_1$ and $t_2$ is:

$$P(T < t_2 | T \geq t_1) \in \left[ \frac{e^{-\overline{\lambda} t_1} - e^{-\overline{\lambda} t_2}}{1 - e^{-\overline{\lambda} t_1}}, \frac{e^{-\underline{\lambda} t_1} - e^{-\underline{\lambda} t_2}}{1 - e^{-\underline{\lambda} t_1}} \right]. \tag{15}$$

### 3.4 Case of periodic preventive maintenance

It is also possible to represent schedules of preventive maintenance by means of probability distributions. Indeed, some components are preventively replaced or repaired with a period of length $\theta$: this maintenance task will reset the probability of failure to 0 after $\theta$ flight hours (FH). The cumulative distribution representing this probability of failure in this case is a periodic function that can be written as:

$$\text{for } k \in \mathbb{N}, P(T < t) = 1 - e^{-\lambda(t - k\theta)}, \text{ if } t \in [k\theta, (k+1)\theta] \tag{16}$$

When the failure rate $\lambda$ is imprecise, then the result is the same as in the section 3.2 on the interval $[0, \theta]$:

$$\text{for } k \in \mathbb{N}, P(T < t) \in [1 - e^{-\overline{\lambda}(t - k\theta)}, 1 - e^{-\underline{\lambda}(t - k\theta)}], \text{ if } t \in [k\theta, (k+1)\theta] \tag{17}$$

If both the failure rate and the period are imprecise, then it is still possible to compute the range of the resulting distribution: we can consider that the period $\theta$ can be any value in the interval of time $[\theta_1, \theta_2]$. In this case, the size of the interval probability will grow very quickly with the size of the interval $[\theta_1, \theta_2]$. The minimum and maximum cumulative distributions, denoted by $\overline{P}(F < t)$ and $\overline{P}(F < t)$, are given for $k \in \mathbb{N}$ by the following expressions:

$$\underline{P}(T < t) = \begin{cases} 0 \text{ for } k\theta_1 < t < k\theta_2 \\ 1 - e^{-\underline{\lambda}(t - k\theta_1)}, \text{ for } t \in [k\theta_2, (k+1)\theta_1] \end{cases}$$

$$\overline{P}(T < t) = 1 - e^{-\overline{\lambda}(t - k\theta_1)}, \text{ for } t \in [k\theta_2, (k+1)\theta_2]$$

An example of those p-boxes for $\lambda \in [0.5, 0.6]$ and $T \in [\theta_1, \theta_2]$ is shown on Fig. 3.

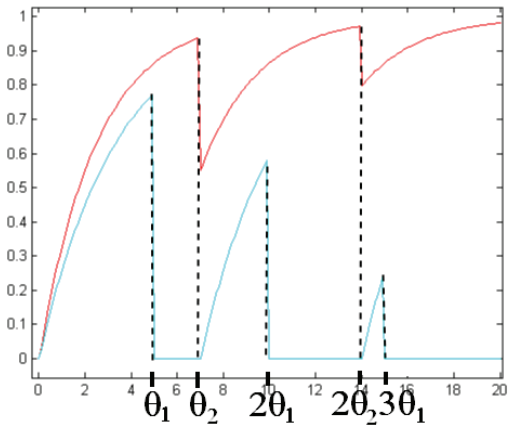



**Fig. 3.** An example of periodic maintenance with $\theta \in [\theta_1, \theta_2]$ and $\lambda \in [0.5, 0.6]$

## 4 Weibull distribution and imprecise parameters

In the case of a hardware component, it can be useful to model its *burn-in* period (i.e. the fact that the failure rate is high at the beginning but will decrease after some time) and its *wear-out* phase (i.e. the fact that after some time, the failure rate of the component increases). Therefore, the failure rate will have the shape of a *bathtub curve*, as shown on Fig.4.

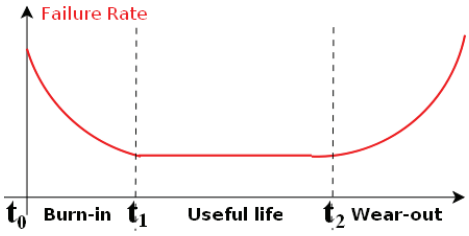



**Fig. 4.** Bathtub Curve

In order to model the reliability in this case, the *Weibull* law is used. It is a two parameters law, described by the formula:

$$R(t) = e^{-(\frac{t}{\eta})^{\beta}} \tag{18}$$

where $\eta$ is the *scale parameter* and $\beta$ the *shape parameter*.

The probability density function of a Weibull law is given by the expression:

$$f_T(t) = \frac{\beta}{\eta}(\frac{t}{\eta})^{\beta-1} e^{-(\frac{t}{\eta})^{\beta}} \tag{19}$$

And its cumulative distribution is:

$$F_T(t) = 1 - e^{-(\frac{t}{\eta})^{\beta}} \tag{20}$$

From equation (5), the expression of the failure rate as a function of $t$ is:

$$\lambda(t) = \beta.\frac{1}{\eta^{\beta}}.t^{\beta-1} \tag{21}$$

To get a bathtub curve, a value $\beta_1 < 1$ is chosen for the burn-in phase ($t_0$ to $t_1$), $\beta = 1$ for the useful life ($t_1$ to $t_2$) and a $\beta_2 > 1$ for the wear-out phase ($> t_2$).

In the wear-out phase, the reference origin of the failure rate and the cumulative function is not 0, hence in order to be able to shift the distribution to starting time $t_2$, a *location parameter* $\gamma$ should be added:

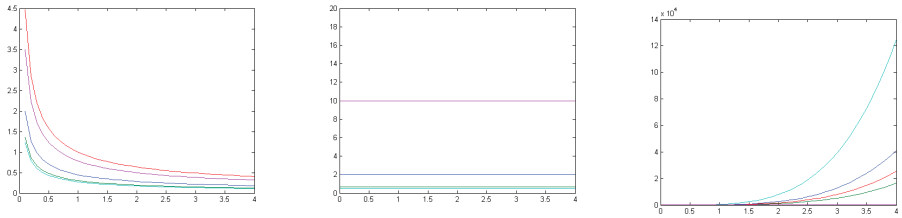
$$F_T(t) = 1 - e^{-(\frac{t-\gamma}{\eta})^{\beta}} \tag{22}$$

Despite the fact that the parameter $\beta$ is different for at each phase of the bathtub curve, the failure rate is a continuous function. Therefore, there will be a constraint for each change of phase, that will ensure the continuity. When the scale parameter $\eta$ remains the same for all the phases, this constraint is expressed as below:

$$\begin{cases} \beta_1.\frac{1}{\eta^{\beta_1}}.t_1^{\beta_1-1} = \frac{1}{\eta} \\ \beta_2.\frac{1}{\eta^{\beta_2}}.(t_2-\gamma)^{\beta_2-1} = \frac{1}{\eta} \end{cases} \Leftrightarrow \begin{cases} \beta_1.(\frac{t_1}{\eta})^{\beta_1-1} = 1 \\ \beta_2.(\frac{(t_2-\gamma)}{\eta})^{\beta_2-1} = 1 \end{cases} \tag{23}$$

Like the failure rate curve, the global cumulative distribution will be composed of three pieces of cumulative distributions with different parameters. To ensure the continuity of the global one, the cumulative distribution of each new phase should start from the last value of the previous phase.

When the parameters of a Weibull law are imprecise, they should still verify the constraints of $\beta$ being less than, greater than, or equal to 1 for each phase, and the ones expressing the continuity of $\lambda(t)$ (equation 23). Fig. 5 shows the variation of the failure rate with the variation of $\eta$, when $\beta$ is fixed, for the three different phases of the bathtub curve.



. a) $\beta_1 < 1$ . b) $\beta = 1$ . c) $\beta_2 > 1$

**Fig. 5.** Variation of the Weibull distribution with $\eta$ for a fixed $\beta$.

The imprecision pervading the parameters of the Weibull law affects the value of the time points where the phases change in the bathtub curve ($t_1$ and $t_2$), due to equation (23). These time points become themselves intervals.

In order to find the range of the cumulative distribution with the different parameters, the monotonicity study of the function will also be required, as in section 3. In this case, we have a two parameter function, hence we compute its gradient.

$$\overrightarrow{\nabla} P(T<t) = \begin{vmatrix} \frac{\partial}{\partial \eta} P(T<t) \\ \frac{\partial}{\partial \beta} P(T<t) \end{vmatrix} = \begin{vmatrix} \beta . \frac{t^\beta}{\eta^{\beta+1}} e^{-(\frac{t}{\eta})^\beta} \\ ln(\frac{t}{\eta}) . (\frac{t}{\eta})^\beta e^{-(\frac{t}{\eta})^\beta} \end{vmatrix} \tag{24}$$

By noticing that $t$, $\eta$, $\beta$ and $e^{-(\frac{t}{\eta})^\beta}$ are always positive, we can conclude that the partial derivative $\frac{\partial}{\partial \eta} P(T<t)$ is positive. But the partial derivative $\frac{\partial}{\partial \beta} P(T<t)$ is positive when $\eta > t$ and negative otherwise, because of the term $ln(\frac{t}{\eta})$. Equation (23) implies that for $\eta > t_1$, hence $P(T<t)$ is decreasing with respect to $\beta$ for $t < t_1$. This means that the p-box of a Weibull distribution will be:

$$[1 - e^{-(\frac{t}{\underline{\eta}})^{\overline{\beta}}}, 1 - e^{-(\frac{t}{\overline{\eta}})^{\underline{\beta}}}], \text{ for } t \in [0, t_1] \tag{25}$$

Between $t_1$ and $t_2$, $\beta$ is fixed to 1, hence the bounds for the cumulative distribution are:

$$[1 - e^{-\frac{t-t_1}{\underline{\eta}}} + P(T<t_1), 1 - e^{-\frac{t-t_1}{\overline{\eta}}} + P(T<t_1)], \text{ for } t \in [t_1, t_2] \tag{26}$$

When $t > t_2$, the quantity $(t_2 - \gamma)$ is computed through equation (23). Now the partial derivatives are similar to the ones in equation (24), replacing $t$ by $t - \gamma$. Hence the condition for $\frac{\partial}{\partial \beta} P(T<t)$ being positive is that $t < \gamma + \eta$, so we get the range of the cumulative distribution:

$$[1 - e^{-(\frac{t-\gamma}{\underline{\eta}})^{\underline{\beta}}} + P(T<t_2), 1 - e^{-(\frac{t-t_2}{\overline{\eta}})^{\overline{\beta}}} + P(T<t_2)], \text{ for } t < \gamma + \eta \tag{27}$$

$$[1 - e^{-(\frac{t-\gamma}{\underline{\eta}})^{\overline{\beta}}} + P(T<t_2), 1 - e^{-(\frac{t-t_2}{\overline{\eta}})^{\underline{\beta}}} + P(T<t_2)], \text{ for } t > \gamma + \eta \tag{28}$$

## 5 Range of a undesired event probability across time

In the case of fault tree analysis, the probability of a undesired event is described with a Boolean formula $F$, function of $N$ Boolean variables $V_i, i = 1 \dots N$ representing the failure (or states) of its components. When the probability of $V_i$ is represented by a probability distribution with an imprecise parameter, we have a p-box for the probability of the undesired event. The variables $V_i$ are supposed to be stochastically independent, and they can follow different probability distributions. Also, their parameters can be of different types: some can be precise, when the information is available and well known, some can be imprecise.

The goal will be to find the p-box describing the undesired event probability across time from the p-boxes of the variables $V_i$. The best way to carry out this computation is to discretize the time, and to find for each $t$ and for each $V_i$, the associated interval $I(t, V_i)$. Of course, if all input probability distributions are precise, the probability of the undesired event will be precise. When $T_i$ is

a random variable representing the failure time of the component $V_i$, we have that:

$$I_i(t, V_i) = [\underline{P(T_i < t)}, \overline{P(T_i < t)}]$$

Let us consider three variables $V_i, i = 1 \ldots 3$, with exponential laws, and respective imprecise parameters $\lambda_1 \in [0.35, 0.45]$, $\lambda_2 \in [0.2, 0.4]$ and $\lambda_3 \in [0.55, 0.6]$. Fig. 6 depicts the intervals $I_i(t = 7, V_i)$ associated to these variables.

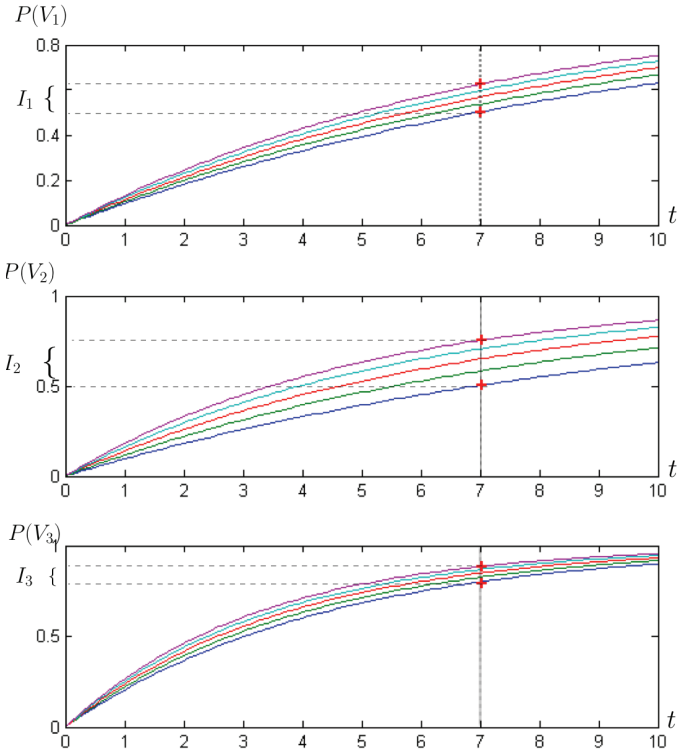



**Fig. 6.** Example of aggregation at $t$ of three exponential p-boxes

For the same time point, the range of the probability of variable $V_i$ is given by the interval $I_i(t, V_i)$. So, *for this time* $t$, the algorithm presented in [1] can be used to compute the probability of the undesired event.

In order to compute the range of the cumulative distribution of the undesired event for *all time instants*, we apply the algorithm for all $k$ time instants, $k = \frac{T_o}{T_s}$, where $T_o$ is the observation interval and $T_s$ is the time step.

### 5.1 Case study: Safety model of a Primary/Backup Switch

In this case study, the analysis process of Safety models used in the @MOST project will be described. We will take the example of a small system allowing a reconfiguration: a Primary/Backup Switch. It is constituted of three components:

– A primary supplier
– A back-up supplier
– A switch that selects the active supplier between the primary or the backup one

When a fault occurs in the Primary supplier, then it switches to the Back-up supplier. But it may also happen that the Switch gets stuck: in this case, it will be impossible to switch to Backup supplier.

The software Cécilia OCAS is used to model the architecture and the behavior of the system thanks to the AltaRica language, which is mode-automata based. From this description, some algorithms [7] will extract fault trees or Minimal Cut Sets for any undesired event selected by the user by means of observers. Fig.7 shows the OCAS model of the Primary/Backup Switch.

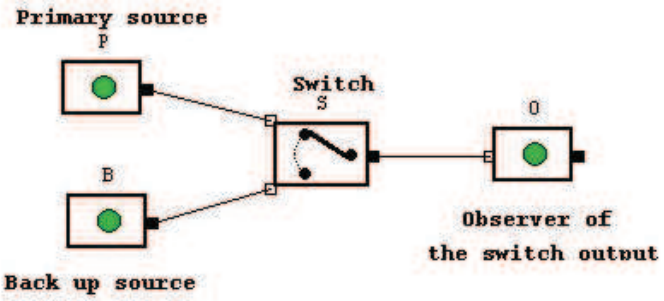



**Fig. 7.** OCAS model of the Primary/Backup Switch

In the following, we will study the undesired event corresponding to the fact that the whole system is down, written as *Obs.KO*. The OCAS tool extracts the fault tree associated to this event, as displayed on Fig.8.

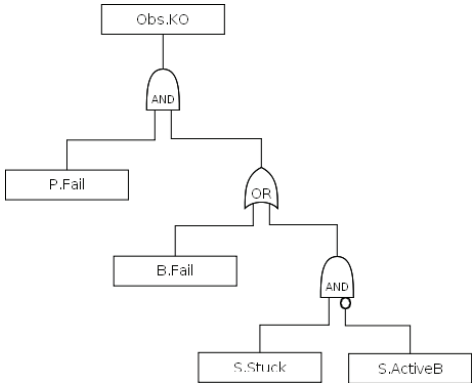



**Fig. 8.** fault tree associated to event *Obs.KO*

Therefore, this fault tree is equivalent to the Boolean formula:

$$Obs.KO = P.Fail \wedge (B.Fail \vee (S.stuck \wedge \neg S.activeB)),$$

where *P.Fail* stands for a failure of the Primary supplier and *B.Fail* for a failure of the Backup supplier. *S.stuck* represents the fact that the Switch is stuck and is not able to activate the Backup, and *S.activeB* is the activation order of the Switch.

The sensitivity analysis algorithm is applied to the fault tree, with the following imprecise parameters for the distributions:

- *P.Fail* possesses an exponential distribution with an imprecise failure rate $\lambda = 10^{-4} +/- 50\%$ and a precise periodic maintenance of period $\theta = 30$ FH
- *B.Fail* possesses an exponential distribution with an imprecise failure rate $\lambda = 10^{-4} +/- 10\%$ and a precise periodic maintenance of period $\theta = 35$ FH
- *S.stuck* possesses an exponential distribution with a precise $\lambda = 10^{-5}$
- An activation order of the Switch occurs after $t = 80$ FH

On Fig. 9, we can observe the minimum and maximum cumulative distributions of the event *Obs.KO*, for a duration of 100 flight hours (around three or four months for a commercial aircraft). The picture lays bare the effect of periodic maintenance on those distributions.

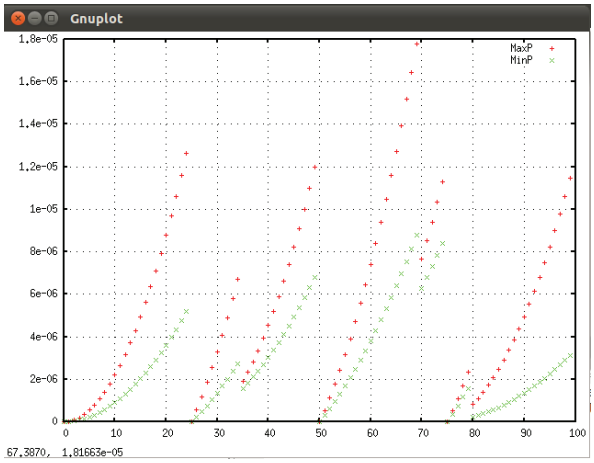



**Fig. 9.** Evolution of the p-box of the event *Obs.KO* for a duration of 100 FHs

The study of this p-box can give crucial information about the probability of undesired events, such as *Obs.KO*: when the area between the minimum curve and the maximum curve is tight, computations are reliable. The larger it is, the more uncertainty we will get. But even under uncertainty, it can still be possible to ensure safety, if the upper probability of the undesired event is below a legal threshold. For instance, in our case study, the maximum probability is always less than $1.8 \times 10^{-5}$ for 100 flight hours, with this maintenance schedule.

In safety analysis, the requirements to meet for each failure are described in the Failure Mode and Effects Analysis document (FMEA, [10]). They are classified with respect to their probability of occurrence, their severity and some other features. This classification defines the legal probability threshold to be

met. In the example, the event *Obs.KO* meets a requirement of an event occurring less than $10^{-4}$ over the 100 first flight hours, but not the threshold of $10^{-5}$. In case a threshold of $10^{-5}$ is required by the FMEA for this event, then we must change the maintenance schedule in order to meet this requirement. The algorithm allows to test easily several scenarios of maintenance, in order to find one that ensures the threshold of $10^{-5}$. With a periodic maintenance of the primary supplier every 19 flight hours instead of 25, and of the backup supplier every 22 flight hours instead of 35, this requirement can be met despite the uncertainty about the inputs, as shown on Fig. 10.

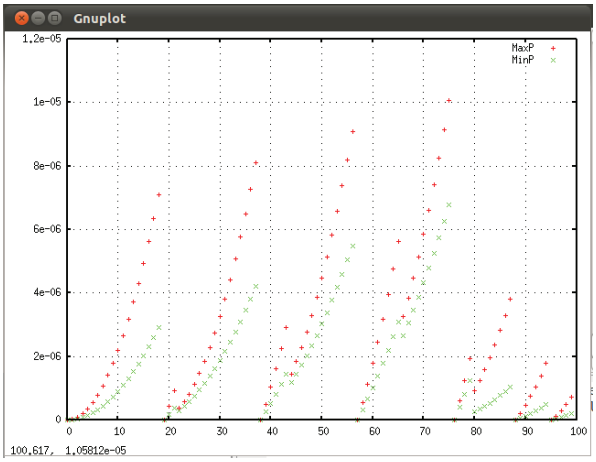



**Fig. 10.** A different scenario of maintenance schedule

The obtained p-box is also compatible with the fuzzy extension of FMEA [11]. In this case, the threshold to meet for occurrence parameter is given by a membership function over an ad hoc scale. After casting the probability interval on such a scale, we can compute the necessity and the plausibility at each time $t$.

## 6 Conclusion

Being able to model the impact of incomplete information on probabilistic safety analysis is very useful for maintenance management. It allows the user to select the best representation for available data, in order to get a faithful advice. Precise data can be used when they are available, but they do not need to be assumed so when they are not. Consequently, more facets of uncertainty can be taken into account, and especially the difference between the variability of failure times and the lack of knowledge on distribution parameters.This difference can be very crucial in a decision process, where confidence about the results of computations plays a decisive role.

The computation time of this algorithm is exponential with respect to logical variables that appears both in positive and negative forms in the fault tree (in

practice there are very few of them [1]). Hence our methodology for risk analysis in maintenance management looks scalable. Further experiments should be run to demonstrate this point.

Future work will take into account the uncertainty of parameters represented by means of fuzzy intervals, using the concept of $\alpha$-cuts ([9]). In fact a fuzzy set can be considered as a collection of nested (classical) intervals, called $\alpha$-cuts. For each $\alpha$-cut, the range of the undesired event is computed. The issue is then to find an algorithm to compose all these ranges into a fuzzy cumulative distribution.

**Acknowledgments.** The authors would like to thank Christel Seguin (ONERA, France) and Chris Papadopoulos (AIRBUS Operations Ltd., UK) for the discussions about the application.

## References

1. C. Jacob, D. Dubois, J. Cardoso: *Uncertainty Handling in Quantitative BDD-Based fault tree Analysis by Interval Computation*, Int. Conf. on Scalable Uncertainty Management, Dayton, Ohio, S. Benferhat, J. Grant (Eds.), Springer, LNCS 6929, p. 205-218, 2011.
2. L. V. Utkin, F. P. A. Coolen: *Imprecise reliability: An introductory overview*, Intelligence in Reliability Engineering, Springer, Vol. 40, p. 261-306, 2007.
3. M. Siegle: *BDD extensions for stochastic transition systems*, Proc. of 13th UK Performance Evaluation Workshop, Ilkley/West Yorkshire, D. Kouvatsos ed, p. 9/1-9/7, July 1997.
4. E. Morice: *Quelques modèles mathématiques de durée de vie*, Revue de statistique appliquée, tome 14, n$^o$1, p. 45-126, 1966.
5. F. Palisson: *Détermination des paramètres du modèle de Weibull à partir de la méthode de l'actuariat*, Revue de statistique appliquée, tome 37, n$^o$ 4, p. 5-39, 1989.
6. S. Ferson, L. Ginzburg, V. Kreinovich, D. Myers, K. Sentz: *Constructing probability boxes and Dempster-Shafer structures*, Tech. rep., Sandia National Laboratories, 2003.
7. A. Rauzy: *Mode automata and their compilation into into fault trees*, Reliability Engineering and System Safety, n$^o$ 78, p. 1-12, 2002.
8. J. Gauthier, X. Leduc, A. Rauzy: *Assessment of Large Automatically Generated Fault Trees by means of Binary Decision Diagrams*, Journal of Risk and Reliability. Professional Engineering, Publishing. Vol. 221, n$^o$ 2, p. 95-105, 2007.
9. L. Zadeh: *Similarity relations and fuzzy orderings*, Information Sciences, Vol. 3, p. 177-200, 1971.
10. D.H. Stamatis: *Failure Mode Effect Analysis: FMEA from theory to execution*, 2nd Edition, 1947.
11. K. M. Tay, C. P. Lim: *A Guided Rule Reduction System for Prioritization of Failures in Fuzzy FMEA*, International Journal of Quality and Reliability Management, Vol. 23 Iss: 8, p.1047 - 1066, 2006.